From: Perlner, Ray (Fed)
To: Peralta, Rene C. (Fed); Liu, Yi-Kai (Fed)
Cc: Jordan, Stephen P (Fed)
Subject: RE: Grover"s algorithm
Date: Tuesday, March 29, 2016 5:25:30 PM

Rene: So I guess by "proportional to P" we simply mean P qubits, and we
have the option of considering them as part of one quantum computer
or of many.
Yes, although I think we still mean Ps qubits or thereabouts
Rene: Since for large P making P quantum computers, each with s qubits, is easier than making one quantum computer with Ps qubits, I mapped
"proportional to P" to "P quantum computers each with s qubits".
It is unlikely that the bound we state holds for this interpretation.
I'm not sure what you mean by this. You absolutely can search for a 2s bit key using P quantum computers each with s qubits in time 2^s/ sqrt(p). Now this may not hold for other, more complicated attacks, but that's a different issue.

From: Peralta, Rene (Fed)
Sent: Tuesday, March 29, 2016 4:44 PM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: Grover's algorithm
Thanks. This must mean that I interpreted what Ray wrote incorrectly.
The question is how fast you can search a space of size 2^(2s) with
resources "proportional to P".
Since for large P making P quantum computers, each with s qubits, is easier than making one quantum computer with Ps qubits, I mapped
"proportional to P" to "P quantum computers each with s qubits".
It is unlikely that the bound we state holds for this interpretation.
So I guess by "proportional to P" we simply mean P qubits, and we
have the option of considering them as part of one quantum computer
or of many. Then the bound holds.
Is this correct?
Regards, Rene.

From: Liu, Yi-Kai (Fed)
Sent: Tuesday, March 29, 2016 2:45 PM
To: Peralta, Rene (Fed)
Cc: Perlner, Ray (Fed); Jordan, Stephen P (Fed)
Subject: Re: Grover's algorithm
Hi Rene,
Sorry I didn't have time to reply earlier! Yes, for Grover's algorithm, if you stop the algorithm early, you can calculate what happens -- Grover's algorithm rotates the state of the system so that it

overlaps partially with the target state, see equation (11) here:
https://courses.cs.washington.edu/courses/cse599d/06wi/lecturenotes12.pdf
You can also ask a related question: what happens to the quantum query lower bounds, when you are operating in this regime where the success probability is very low? Mark Zhandry has some results about this -- for instance, he shows that for unstructured search over N items using q queries, the best success probability is O(q^2/N), see here:
https://www.cs.princeton.edu/~mzhandry/docs/talks/QSol.slides.pdf
Cheers,
--Yi-Kai

From: Peralta, Rene (Fed)
Sent: Monday, March 28, 2016 2:35 PM
To: Liu, Yi-Kai (Fed)
Cc: Peralta, Rene (Fed)
Subject: Grover's algorithm
Hi Yi-Kai,
In Grover's algorithm (for a space of size N) one iterates
calls to two operators about sqrt(N) times, then one measures
and obtains the target with probability about 1. What happens
if you do fewer iterations and then measure? How does the
probability decay?
Thanks, Rene.